
NCSEA
Nationale Cyber Security Educatie Agenda
dcypher

Voorwoord

Bij de oprichting kreeg dcypher (dutch cybersecurity platform higher education & research) ook een hoger onderwijsopdracht mee. De uitdagingen om goed en passend hoger onderwijs in cybersecurity te bieden zijn groot. Om daarop meer grip te krijgen heeft dcypher in de afgelopen vier jaren verschillende activiteiten ontplooid. Eén zo'n activiteit was een werkontbijt over cybersecurity onderwijs op 30 juni 2017, dat dcypher samen met het ministerie van Justitie en Veiligheid organiseerde. De ontoereikende aandacht voor cybersecurity in het onderwijs, die in het rapport 'De economische en maatschappelijke noodzaak van meer cybersecurity - Nederland digitaal droge voeten' (2016)[1] gemeld werd, was aanleiding dit te organiseren.

Herna Verhagen (CEO PostNL en auteur van dit adviesrapport) was een van de deelnemers. Voor het dcypher Magazine 2018[2] werd naar haar indrukken gevraagd van wat tijdens het ontbijt ter sprake kwam: *'Ik vond het opvallend te horen hoeveel verschillende acties er al lopen op het terrein van cybersecurity onderwijs en bewustwording. Het landschap is echter wel erg fragmentarisch: er zijn veel spelers die niet op de hoogte zijn van elkaar en elkaars initiatieven. Met een gezamenlijk plan kunnen die inspanningen veel meer kracht krijgen. Ik ben er voorstander van dat het onderwijsveld een gezamenlijke onderwijsagenda opstelt en verwezenlijkt.* ***dcypher kan hier een rol bij spelen door samenwerking te stimuleren en aan te jagen, en verschillende initiatieven met elkaar te verbinden.'***

Aan die oproep is gehoor gegeven: dcypher heeft talloze gesprekken gevoerd, initiatieven genomen, en aan de onderwijstaak gerelateerde, zowel lopende als nog te starten initiatieven bijeengebracht. Tezamen vormen deze een reeks van interventies. Deze reeks vormt de kern van deze Nationale Cyber Security Educatie Agenda. Waar mogelijk zijn interventies onderling logisch met elkaar verbonden.

Wat mooi zou het zijn als we over vijf jaar kunnen zeggen: 'Nederland zag de uitdaging en realiseerde de daarbij behorende ambities'.

Inhoudsopgave

Leeswijzer

Dit document bestaat globaal uit drie delen:

1. Het eerste deel begint met het benoemen van de aanleiding voor het uitbrengen van deze agenda, gevolgd door een achtergrond en contextbeschrijving. Uiteengezet wordt wat dcypher gaandeweg is gaan verstaan onder agendering van cybersecurity hoger onderwijs. Scope en doelgroep van de agenda worden in dit deel gedefinieerd. Ondersteund door een infographic wordt vervolgens het kwantitatieve en kwalitatieve tekort aan mensen met cybersecuritykennis en -vaardigheden in Nederland 'geagendeerd'. Het gaat hier om zowel cybersecurity experts als om beroepsgroepen waar aspecten van cybersecurity een rol spelen. De huidige mismatch tussen (arbeidsmarkt-) vraag en (hoger onderwijs-) aanbod kan alleen opgelost worden als onderwijs, publieke en private sector structureel samenwerken. Dit deel vormt zo de opmaat naar wat volgt.
2. Het tweede deel betreft een lijst van interventies in het cybersecurity (hoger) onderwijs. Hiermee wordt een overzicht gegeven van er op dit moment in diverse 'triple helix' samenwerkingen gebeurt en wat er de komende jaren gedaan moet worden door onderwijs, private én publieke partijen, om tijdelijke en uiteindelijk structurele verbeteringen te kunnen bewerkstelligen. De interventies zijn verdeeld over zes hoofdthema's. Vier van deze thema's (professionaliseren, doceren, samenwerken en verbreden) hebben betrekking op het hoger onderwijs en vormen de kern. De andere twee thema's (voorbereiden en interesseren) hebben grotendeels betrekking op het primair en voorgezet onderwijs en het mbo. Hieronder vallende interventies moeten gezien worden als randvoorwaardelijk voor de in- en doorstroom naar het hoger onderwijs. N.b. De lijst met interventies is een 'levend' overzicht, dat met het voortschrijden van tijd en inzicht kan veranderen. Het is niet bedoeld als roadmap; voor prioritering en uitvoering van het geheel aan interventies is regievoering aan te bevelen.
3. In een bijlage wordt de volle breedte van dcyphers hoger onderwijs-opdracht belicht. Daarin wordt een overzicht gegeven van de hoger onderwijsactiviteiten door dcypher in de periode 2016-2020. Met de drie delen tezamen legt dcypher verantwoording af over de hoger onderwijs-opdracht die het in 2016 meekreeg. Tenslotte volgen een lijst van in dit document gebruikte afkortingen en een lijst met referenties.

De uitdaging

De toenemende digitalisering van de maatschappij creëert een groeiende behoefte aan mensen met kennis en expertise op het gebied van digitale veiligheid. De afhankelijkheid van ICT betekent dat iedere burger over basiskennis van ICT moet beschikken en digitaal weerbaar moet zijn, dat onderwijs op dit terrein al op jonge leeftijd moet beginnen en dat cybersecurity onderwijs op alle niveaus en in alle studierichtingen noodzakelijk is.[3]

De urgentie

Ontwikkelingen op het terrein van digitalisering gaan razendsnel en digitalisering is tot in de haarvaten van onze samenleving doorgedrongen. Het opleiden of omscholen van mensen die de veiligheidsaspecten van deze ontwikkeling adequaat en efficiënt kunnen adresseren, zowel op technisch als op sociaal-wetenschappelijk en geesteswetenschappelijk vlak, blijft ver achter, zowel in aantallen (kwantitatief) als in kennisniveaus (kwalitatief). Het aldus ontstane gat op de arbeidsmarkt tussen de vraag naar en het aanbod van cybersecurity expertise, op alle terreinen, niet alleen technisch, maar ook bijvoorbeeld organisatorisch, bestuurlijk, juridisch, economisch en ethisch, is de directe aanleiding voor het uitbrengen van deze agenda.

Dagelijks ondervinden wij de gevolgen van niet goed werkende, onveilige technologie of het onveilige gebruik ervan. De consequenties kunnen economisch, sociaal, maatschappelijk, technisch, juridisch en politiek zijn. De dreiging van beroepscriminelen en statelijke actoren in het cyberdomein neemt toe, terwijl de aanvallen ook steeds geavanceerder en complexer worden. In 2012 werd de schade voor de Nederlandse samenleving door cybercriminaliteit al geschat op jaarlijks minimaal 10 miljard euro. Toen ging het o.a. om industriële spionage, fraude, afpersing en phishing.[4] De situatie is anno 2020 echter veel complexer en urgenter.

Het Centrum Informatiebeveiliging en Privacybescherming (CIP)[5] waarschuwt dat een samenleving zich geen Internet of Things kan veroorloven zonder aandacht voor integrale beveiliging. De risico's voor burgers, de bedrijfsvoering en onze economie zijn daarvoor te groot. De Algemene Rekenkamer[6] doet een reeks van aanbevelingen voor de vitale waterwerken, zoals het in beeld brengen van het actuele cybersecurity-dreigingsniveau, de detectie op cyberaanvallen bij vitale waterwerken en het niveau van screening voor SOC-medewerkers. De NCTV[7] bevestigt dat de digitale dreiging voor de nationale veiligheid permanent is. Vrijwel alle vitale processen en systemen in Nederland zijn deels of volledig gedigitaliseerd, waarbij er nauwelijks terugvalopties of analoge alternatieven zijn. Ook de Wetenschappelijke Raad voor het Regeringsbeleid[8] (WRR) waarschuwt dat de samenleving in korte tijd zó snel is gedigitaliseerd dat er onverantwoorde risico's zijn ontstaan: Nederland is kwetsbaar voor digitale aanvallen. De WRR pleit voor een betere voorbereiding op digitale ontwrichting. De coronapandemie, en het daarmee gepaard gaande massale thuiswerken, laat eens te meer zien hoe groot de afhankelijkheid is van een veilige en privacy waarborgende digitale infrastructuur voor alle burgers.

Om digitale ontwrichting te voorkomen en schade te beperken bij incidenten, moeten in een groot deel van de samenleving capaciteiten opgebouwd worden. 'Capacity building' is daarom een kernbegrip voor cyberveiligheid.

> **Kennis- en innovatieagenda Veiligheid, oktober 2019** [9]


prijslijst
Team Hangout Hogeschool
CTC
Coca-Cola
Nutella
Ferrero
Ferrero Rocher
Duc d'O
Penotti
Lipton
Coca-Cola

dcypher en de agendering van het cybersecurity hoger onderwijs

Het Dutch Cybersecurity Platform Higher Education & Research (dcypher) kreeg naast een onderzoekopdracht een hoger onderwijsopdracht mee. Ook de naam van dit platform verwijst daar naar. In de twee subsidiebeschikkingen (2016 en 2018) wordt de hoger onderwijstaak als volgt omschreven: *Ontwikkeling van een agenda/manifest voor cybersecurity hoger onderwijs (inclusief veldraadplegingen).*

Het in 2016 door de ministeries van J&V, OCW, EZK en NWO opgerichte dcypher kreeg naast een opdracht op het gebied van cybersecurity onderzoek ook een cybersecurity hoger onderwijs opdracht mee.
> **Nederlandse Cybersecurity Agenda, Ministerie van J&V, april 2018**[10]

In het meerjarenbeleidsplan uit 2016 formuleert dcypher als zijn visie: *Nederland positioneert zich als een land dat, op het terrein van cybersecurity, excellente wetenschap bedrijft, uitstekend (hoger) onderwijs biedt, door onderzoek verkregen (academische) kennis en kunde ten goede laat komen aan het innovatief vermogen van de publieke en private sector en aan deze sectoren uitstekende hoogopgeleide professionals aflevert.*

Het platform dcypher heeft een agenderende en faciliterende taak voor wat betreft het (wetenschappelijk en praktijkgericht) cybersecurity onderzoek en hoger onderwijs. In het leggen van verbindingen in de kennis- en innovatieketen treedt dcypher ook coördinerend op.
Met de publicatie van de NCSRA-III[11] in 2018, bouwt dcypher voort op een traditie van bottom-up agendering van cybersecurity onderzoek in Nederland die begon in 2007. Agendering van het hoger onderwijs in cybersecurity kent echter geen traditie waarop kan worden voortgebouwd.

Deze onderwijsagenda is dus te beschouwen als **invulling van de agenderende taak betreffende het cybersecurity hoger onderwijs**. Omdat het hoger onderwijs niet op zichzelf staat, wordt uitdrukkelijk ook de verbinding gelegd met de onderliggende basis, dat wil zeggen het primair onderwijs, voortgezet onderwijs en het mbo.

Naast een NCSRA ook een NCSEA

Belangrijk is de verwevenheid van cybersecurity onderzoek en onderwijs te benadrukken. Resultaten van onderzoek, waarvoor de NCSRA het kader is, worden verspreid via verschillende media. Kennisdisseminatie vindt allereerst plaats in de kennisinstelling waar de nieuwe kennis is ontwikkeld. Die kennis sijpelt door in het onderwijscurriculum, bijvoorbeeld in de universitaire masterprogramma's. In dit proces zien we een intra-universitaire vermenigvuldigingsfactor. Eén PhD-project leidt geregeld tot kennis-verspreiding onder honderden masterstudenten.

De verwevenheid van onderwijs en onderzoek is een kracht, maar staat onder druk. Een sterk punt van het hoger onderwijs in Nederland is de samenhang tussen onderwijs en onderzoek (Financiën, 2014; KNAW, 2019). Hierdoor ontwikkelen studenten in Nederland een onderzoekende houding, leren ze creatief denken en worden ze gestimuleerd om nieuwe wegen te verkennen. Onderzoek verbetert ook de inhoud van het onderwijs, doordat recente inzichten en innovaties in het onderwijs een plek krijgen.

> Strategische agenda hoger onderwijs en onderzoek, Ministerie van OCW, december 2019 [12]

Omdat er geen traditie was in agendering van cybersecurity hoger onderwijs vormde de interpretatie van de aan dcypher opgedragen onderwijstaak een uitdaging. Vragen als: Wat wordt met een hoger onderwijs agenda bedoeld?, Wat is de scope?, Wie draagt of dragen verantwoordelijkheid voor de uitvoering? vroegen om beantwoording.

Na uitgebreide veldraadpleging en consultatie van de dcypher Adviesraad zijn we uitgekomen op een agenda die in de kern bestaat uit een **reeks interventies**, die nieuwe en bestaande initiatieven bijeen brengt en met elkaar verbindt. Een interventie in deze context definiëren we als één of een serie geplande **veranderingsactiviteiten**. Deze zijn gericht op het verkleinen van het kwalitatieve en kwantitatieve tekort aan cyber(security) competenties (ofwel kennis en vaardigheden op het gebied van digitale veiligheid).

Net als voor de **onderzoeksagenda** kiezen we voor de **hoger onderwijsagenda** een nationale aanpak en positionering, een agenda die (onder andere) doorsnijdend is voor (economische) topsectoren en diverse NWA-routes. Het is ook een agenda die te beschouwen is als deelinvulling van topsector gerelateerde Human Capital Agenda's (HCA's). Alle topsectoren hebben immers raakvlakken met cybersecurity.
In de Roadmap Human Capital 2020 - 2023[13] geven de topsectoren aan zowel onderling als met andere partners op het terrein van Human Capital[I] de samenwerking te willen versterken.

De missie van de topsectoren is een 'toekomstbehendige' beroeps-bevolking als voorwaarde voor een florerende economie en een positieve maatschappelijke dynamiek. Alle topsectoren werken zowel vanuit het perspectief van bedrijven als van professionals en vak-mensen. In hun human capital-agenda's staat de discrepantie tussen de behoefte van bedrijven aan voldoende goed opgeleid personeel en de beschikbaarheid van deze mensen centraal. Ook de ontwikkelmogelijk-heden voor professionals en vakmensen spelen een belangrijke rol: hoe kunnen zij zich (toekomstgericht) blijven ontwikkelen?

> Samen aan de slag - Roadmap Human Capital 2020 - 2023 van de topsectoren

I. Met 'Human Capital' worden competenties, kennis, sociale vaardigheden en persoonlijkheidskenmerken bedoeld, die mensen in staat stellen waarde te creëren.

Als naam voor deze dcypher hoger onderwijsagenda is gekozen voor NCSEA, ofwel Nationale Cyber Security Educatie Agenda. De verwantschap in naamgeving met die andere dcypher agenda, de NCSRA, is niet toevallig. De doelstelling en insteek is echter anders. Centraal in de NCSEA staat het arbeidsmarktvraagstuk van mismatch tussen vraag naar en aanbod van hoger geschoold personeel met kennis van cybersecurity, in zowel kwantitatief als kwalitatief opzicht. Aan de vraagkant wordt niet alleen gekeken naar de cybersecurity beroepsgroep (de experts), maar ook naar alle vakgebieden waar kennis van cybersecurity steeds belangrijker wordt. Aan de aanbodkant ligt de focus op de uitstroom uit het hoger onderwijs.

Capaciteitsopbouw van cybersecurity professionals.
Cybersecuritykennis is niet alleen voorbehouden aan de cybersecurity beroepsgroep. Ook cybersecurity-competenties binnen andere beroepen worden door verdergaande digitalisering belangrijker. Daarmee wordt toevoeging van deze competenties aan onderwijscurricula van belang. Dit alles moet leiden tot een pakket aan concrete korte en lange termijn maatregelen gericht op verdere structurering en professionalisering van het:

1. vakgebied: een heldere definitie van (harde en zachte) cybersecurity-competenties, eenduidige (internationaal afgestemde) certificering van cybersecurity professionals, duidelijke en aantrekkelijke arbeidsvoorwaarden en loopbaanpaden.
2. kennisgebied: een algemeen geaccepteerde body of knowledge en een cybersecurity lexicon, voldoende gekwalificeerde docenten en meer samenhang binnen het cybersecurity onderwijs.
3. toepassingsgebied: meer samenwerking aan de vraagzijde van de arbeidsmarkt, waar cybersecuritykennis wordt toegepast en geborgd in een breed spectrum van vakgebieden, en waar binnen organisaties vergroting gewenst is van de cybersecurity compliance.

Kennis- en innovatieagenda Veiligheid, oktober 2019

Scope en doelgroep

Zoals hiervoor al opgemerkt ligt de focus in deze agenda op het hoger onderwijs (hbo, wo) in Nederland, opdat het voldoende cybersecurity-professionals aflevert, zowel in kwalitatieve als in kwantitatieve zin, en dat het cybersecuritykennis in aanpalende vakgebieden versterkt.
Ook "Leven lang leren"[II] is onderdeel van het dichten van het eerder genoemde gat op de arbeidsmarkt en daarmee van deze agenda.
Werkenden realiseren zich in toenemende mate dat ze met hun Master diploma in een sterk veranderende realiteit na een aantal jaren bijscholing behoeven, juist en zeker ook op het terrein van cybersecurity. Natuurlijk zijn er talloze korte cursussen en certificaten te behalen in de markt om aan deze vraag te voldoen. Maar we zien ook dat werkenden steeds vaker aankloppen bij hbo's en universiteiten voor post-hbo en post-wo onderwijs, in allerlei soorten en maten (van modulair en online tot complete deeltijd-opleidingen) en dat een "Leven lang leren" steeds duidelijker als vraag en ambitie op de bestuurderstafels van het Nederlands hoger onderwijs komt te liggen.
De doorstroommogelijkheid van het mbo naar het hbo is een aandachtspunt. Het versterken van cybersecuritykennis in primair - en voortgezet onderwijs, als onderdeel van digitale (basis-)vaardigheden, is randvoorwaardelijk voor het behalen van de doelstellingen in het vervolgonderwijs.

Uitvoering van de verderop in deze agenda opgenomen interventies moet bewerkstelligen dat er evenwicht is tussen de behoefte aan voldoende gekwalificeerd personeel met cybersecurity-competenties op de arbeids-markt en het aanbod vanuit het hoger onderwijs.

De (potentiële) uitvoerders van die interventies vormen de primaire doelgroep van deze agenda.
Ook beleidsmakers kunnen tot de doelgroep worden gerekend.
Veel interventies zijn gericht op samenwerking van het hoger onderwijs, bedrijven, overheden en het beroepenveld (binnen het onderwijs, bedrijven en overheden). Tezamen vormen zij de triple helix.

'Onderwijsinstellingen dragen een verantwoordelijkheid om te zorgen voor opleidingsaanbod dat voldoet aan de vraag van de arbeidsmarkt. Een capaciteitsbeperking voor een opleiding die opleidt voor een sector met groot arbeidsmarkttekort is dan ook onwenselijk. Maar de verantwoordelijkheid ligt niet alleen bij de instellingen. Er ligt ook een rol voor werkgevers om een bijdrage te leveren aan het aantrekkelijk maken van werken in de sector.'

> Strategische agenda hoger onderwijs en onderzoek, Ministerie van OCW, december 2019

II. Soms aangeduid als: "Leven lang ontwikkelen".

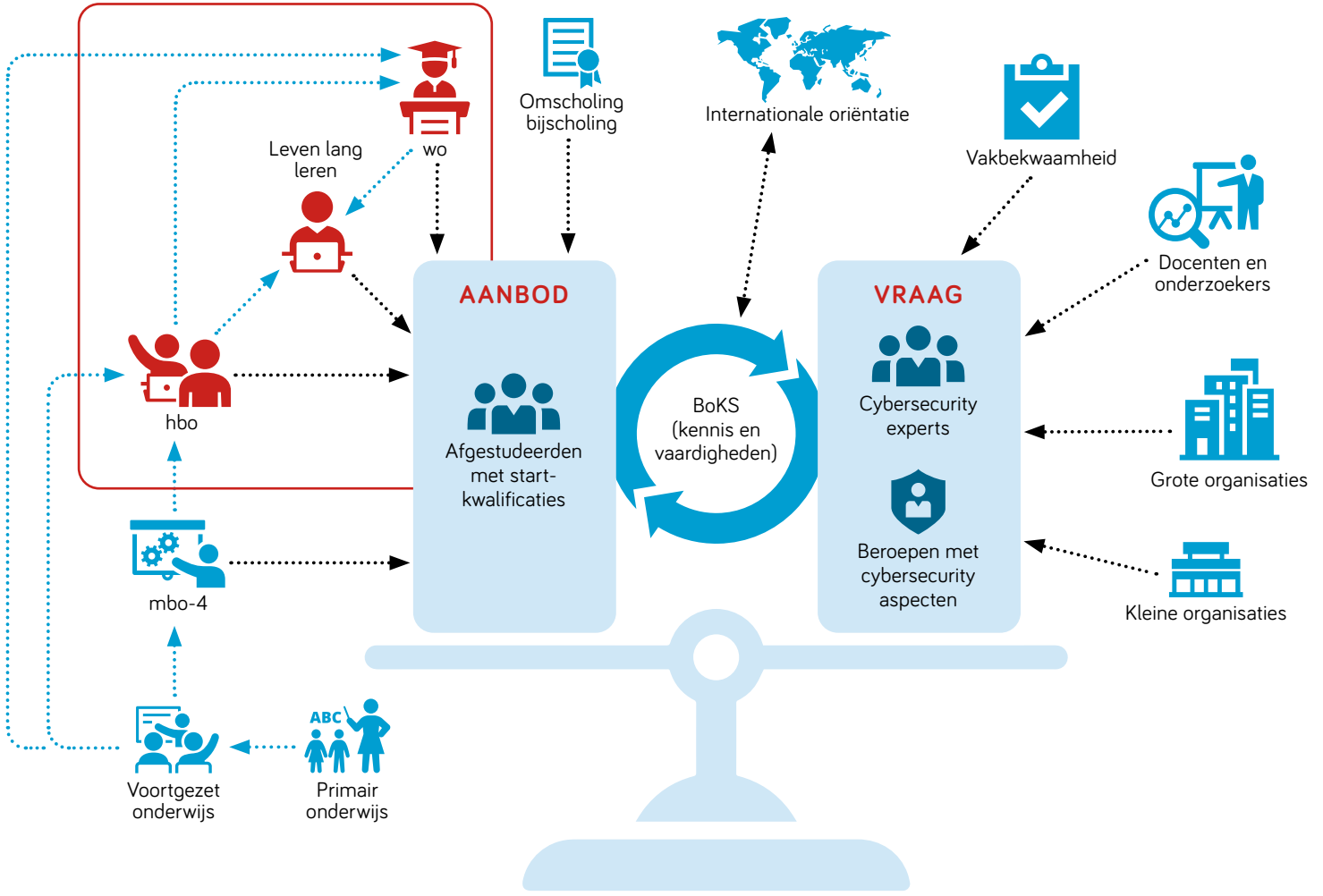
Balans tussen arbeidsmarkt en onderwijs

Alvorens de vraag naar cybersecurityprofessionals uit de arbeidsmarkt te kunnen vergelijken met het aanbod c.q. de uitstroom uit het onderwijs, heeft dcypher het cybersecurity hoger onderwijs in Nederland in kaart gebracht en via de dcypher website[14] ontsloten.

Onderzoek onder stakeholders uit het onderwijs, de publieke en de private sector naar de behoefte(n) van de arbeidsmarkt, bevestigen een toenemend (kwalitatief en kwantitatief) tekort aan cybersecuritykennis en -expertise.[15] Dit betreft niet alleen specialistische cybersecurity expertise, maar ook basisvaardigheden en aan (andere) vakgebieden gerelateerde cybersecuritykennis. Hierdoor is er onvoldoende cybersecuritykennis binnen organisaties, die daardoor minder weerbaar zijn bij actuele digitale dreigingen. Professionalisering van de beroepsbevolking op het gebied van cybersecurity wordt daarom steeds urgenter: er moeten voldoende mensen zijn die beschikken over de voor hun beroep of vakgebied noodzakelijke cybersecuritykennis en -vaardigheden.
In de aanpak van de (kwantitatieve en kwalitatieve) mismatch tussen de vraag naar en het aanbod van cybersecurity-competenties (kennis en vaardigheden) wordt een model gehanteerd voor de balans tussen beide. Dit model, als infographic weergegeven, biedt een overzicht van het totale speelveld.

Uitvoering van de verschillende interventies (waartussen meer of minder samenhang bestaat of kan worden gerealiseerd) draagt bij aan het bereiken van het gewenste evenwicht tussen vraag en aanbod.

Figuur 1. De kwantitatieve en kwalitatieve balans tussen onderwijsaanbod en arbeidsmarktvraag m.b.t. cybersecuritykennis en -vaardigheden



Toelichting op de infographic:

1. De actuele marktvraag naar cybersecuritykennis en -vaardigheden (vakbekwaamheid) wordt gespecificeerd door de arbeidsmarkt (publieke en private, kleine en grote organisaties, waaronder de onderwijs- en kennisinstellingen met hun behoefte aan docenten en onderzoekers).
2. Een startkwalificatie (aan de aanbodzijde) wordt door de Nederlandse overheid gezien als het minimale onderwijsniveau dat nodig is om serieus kans te maken op duurzaam geschoold werk in Nederland.
3. De aansluiting van het onderwijsaanbod op de marktvraag draait in kwalitatieve zin om kennis en vaardigheden, ofwel de startkwalificaties die aansluiten op gestelde vakbekwaamheidseisen. In de beroepspraktijk worden deze verder ontwikkeld tot specifieke kennis en vaardigheden afgestemd op functies. Voorbeeld: Het door het Ministerie van OCW goedgekeurde curriculum van de mbo-opleiding ICT beheer (niveau 4) voldoet vanaf september 2020 aan de startkwalificaties voor ICT Security Specialist[16]. In kwantitatieve zin draait het om voldoende aantallen afgestudeerden.
4. Leerlingen in het primair en voortgezet onderwijs worden voorbereid op veilig, verantwoord en zelfstandig handelen in het digitale domein (21st century skills).[17]
5. Het roodomlijnde deel in de figuur heeft betrekking op het hoger onderwijs (hbo, wo en post-hbo en post-wo trajecten, zie verderop).
6. Van het hoger onderwijs (hbo en wo) komt een voldoende aantal afgestudeerden met de vereiste startkwalificaties voor vakbekwaamheid.[18] In het curriculum blijft ruimte om naar eigen inzicht te voorzien in de specifieke behoefte aan kennis en vaardigheden van de arbeidsmarkt in regio's en voor ontwikkeling van academische competenties (die horen bij een zich snel ontwikkelend onderzoeksterrein).
7. Omscholing en bijscholing van werkenden beïnvloedt de kwaliteit en kwantiteit van zij-instromers.
8. Omscholing en bijscholing op hoger onderwijsniveau wordt aangeduid als "leven lang leren", continuous professional education, post-hbo en post-wo trajecten. Werkenden, die bijvoorbeeld een post master in cybersecurity volgen, komen veelal in de cybersecurity sector terecht, waar ze aanvankelijk niet werkten. Dit is nu weliswaar een klein aantal, maar de verwachting is dat dit aantal in de komende jaren stijgt. Vergelijk het met de "zij-instromers" die in de jaren '90 en '00 zijn overgestapt uit allerlei beroepsgroepen naar de IT.

Van belang is dat de samenwerking tussen instellingen en de dialoog met maatschappelijke partners structureel is ingebed. Het onderhouden van een horizontale dialoog met de buitenwacht is een belangrijke voorwaarde voor, of zelfs een kenmerk van, onderwijskwaliteit.

> Strategische agenda hoger onderwijs en onderzoek, Ministerie van OCW, december 2019

Het nationale overheidsbeleid

Het beleid van de Nederlandse overheid anticipeert op de huidige mismatch[19]. Het draagvlak om het beleid uit te voeren is geconcretiseerd in de Kennis- en Innovatieagenda Sleuteltechnologieën 2020-2023[20] en de Missies voor het topsectoren- en innovatiebeleid[21]. Het beleid adresseert de kwalitatieve en kwantitatieve mismatch. De NCSEA:

a. is ontwikkeld in aansluiting op, of als nadere invulling van, (beleids) voornemens zoals voortkomend in de NCSA en strategieën van de ministeries van OCW, Defensie en EZK;
b. sluit aan bij de Nederlandse ambities op het gebied van cybersecurity;
c. onderschrijft het belang van "leven lang leren". De rol die het hoger onderwijs daarin zal gaan spelen wordt belangrijker in de komende jaren. Dat geldt zeker op het terrein van cybersecurity, waar kennis en capaciteiten snel verouderen en steeds nieuwe uitdagingen, nieuwe technologieën, nieuwe methodieken en theorieën opkomen;
d. houdt rekening met ontwikkelingen in het buitenland omdat landsgrenzen in de cyberwereld nauwelijks een rol spelen.

… Deze ontwikkelingen zullen in de komende jaren een beroep doen op al het beschikbare arbeidspotentieel in deze sectoren. We hebben alle talent nodig en dat vraagt om een arbeidsmarkt die ruimte biedt, talent helpt ontwikkelen en iedereen in staat stelt om naar eigen vermogen deel te nemen. Daarbij geldt dat leren en opleiden al lang niet meer een zaak is van uitsluitend een initiële opleiding. Het aanpassingsvermogen van mensen én organisaties wordt op de proef gesteld. Iedereen moet zich blijven ontwikkelen zodat we de uitdagingen van de toekomst aankunnen.

> Samen aan de slag – Roadmap Human Capital Topsectoren 2020-2023, november 2019

Om de kracht van ons stelsel in stand te houden is meer samenwerking tussen overheid en hogeronderwijsinstellingen, en tussen hogeronderwijsinstellingen onderling, nodig.

> Strategische agenda hoger onderwijs en onderzoek, Ministerie van OCW, december 2019

Internationaal

Wereldwijd is als gevolg van toenemende digitalisering, cybersecurity incidenten, wetgeving en de ontwikkeling van ICT, de vraag naar cybersecurity professionals toegenomen. De mate, schaal en aard van de tekorten kan echter niet eenduidig worden vastgesteld[22]. Voor de discussie over de rol van het onderwijssysteem bij het voorbereiden van studenten op de arbeidsmarkt, is overeenstemming nodig over de kennis en vaardigheden (BoKS = Body of Knowledge and Skills) en over wie de verantwoordelijkheid neemt voor welke rollen bij het ontwikkelen ervan. Werkgevers hebben hier ook een rol in. Internationale overheden hebben vooral geïnvesteerd in het hoger onderwijs, onderzoek en stimulering van de ontwikkeling van personeel. Australië, Frankrijk, de UK en de US hebben tevens ervaring met certificatieschema's voor nationale cybersecurity opleidingen[23].

Meer samenwerking, ook binnen Europa, en bundeling van krachten, zijn nodig om bij te dragen aan de regionale samenleving en economie en om mee kunnen doen met de wereldtop van onderwijs en onderzoek. Hogescholen dienen in de gelegenheid te worden gesteld om het praktijkgerichte onderzoek te versterken.

> **Strategische agenda hoger onderwijs en onderzoek, Ministerie van OCW, december 201**

ECSO's European Human Resources Network for Cyber Task Force creates awareness among decision makers (private companies, regional / local administrations, national / EU administrations) about the need to develop education and training measures which will address the demand in the cyber security field. The target is to increase public and private spending in the relevant field to foster more possibilities of such education and training that recruiters are looking for, both in private and public sectors. Our focus is on professionalisation of cybersecurity professionals.

> **EHR4CYBER Task Force[24]**

Uitvoering van deze agenda onder regievoering

Deze agenda is actiegericht. Er zijn interventies gedefinieerd die in samenhang tot verbetering zullen leiden. Er zijn ook interventies die bij afzonderlijke uitvoering impact hebben. De interventies verschillen in omvang, looptijd en complexiteit. Aan de interventies wordt door zowel onderwijs, overheden als ondernemingen deelgenomen. Er is gekozen voor een actiegerichte benadering, omdat:

a. de urgentie van de problematiek evident is en de situatie dringend verbetering behoeft;
b. het continu veranderende dreigingsbeeld en de noodzaak met nieuwe kennis daarmee in de pas te blijven lopen, om een praktische aanpak vragen;
c. van nieuwe analyses (zoals naar de mate, schaal en aard van de tekorten) weinig toegevoegde waarde kan worden verwacht en concrete en voortvarende actie vertraagt en in de weg staat.

De aard van de interventies van deze agenda kan verschillen.
Er zijn interventies die:

- een eigenaar hebben en al in uitvoering zijn;
- nog een eigenaar moeten krijgen;
- op korte termijn tot resultaten zullen leiden;
- een lange voorbereidingstijd nodig hebben en pas op lange termijn tot resultaten leiden;
- op korte termijn gestart kunnen worden, maar ook tot structurele verbetering leiden;
- zeer zichtbaar zijn en een voorbeeldfunctie kunnen vervullen, aanjager zijn voor opvolgende actie of interventie;
- betrokkenheid van het onderwijs verlangen, met inachtneming van de eigen verantwoordelijkheid, wetenschappelijke vrijheid en mate van autonomie.

Elke interventie behoeft een eigenaar/eindverantwoordelijke met een projectdoel en een projectplan.
Interventies kunnen verschillende eigenaren (verantwoordelijken voor de uitvoering) hebben.
Eén of meer actoren voeren de interventie uit. Daarbij kunnen één of meer partijen betrokken zijn.
Alle interventies dragen op kortere of langere termijn bij aan het verbeteren van de kwalitatieve en kwantitatieve balans tussen vraag en aanbod.
Van eigenaren wordt verwacht dat zij samen met de actoren de interventies volgen, periodiek de effectiviteit en de resultaten interpreteren, en zonodig doelen en acties bijsturen en/of herijken. Het actief volgen en zonodig aanpassen van interventies houdt de actoren gemotiveerd bij het veranderingsproces betrokken te blijven.

Centrale onafhankelijke **regievoering** over uitvoering van het geheel van de interventies is aan te bevelen. Het bevordert samenhang en samenwerking en voorkomt fragmentatie. Regie is evenzeer nodig om inzicht te bereiken of de mate, schaal en aard van de tekorten zich richting de gestelde doelen ontwikkelen. Dit houdt in het monitoren van (tussen)resultaten van de interventies. Ook zal duidelijk moeten zijn op welke wijze en met welke instrumenten het gewenste evenwicht tussen vraag en aanbod voor cybersecurity geborgd kan worden. Institutionalisering van deze regierol zou deel moeten uitmaken van het “hoger plan”, zoals hieronder genoemd.

... kennis en kunde op het terrein van cybersecurity blijven achter. Er is een schreeuwend tekort aan goed geschoolde professionals, zowel bij de overheid als in de wetenschap en in de private sector. Door tekorten aan mensen en middelen kan het hoger onderwijs onvoldoende studenten opleiden om de gaten te dichten.

...

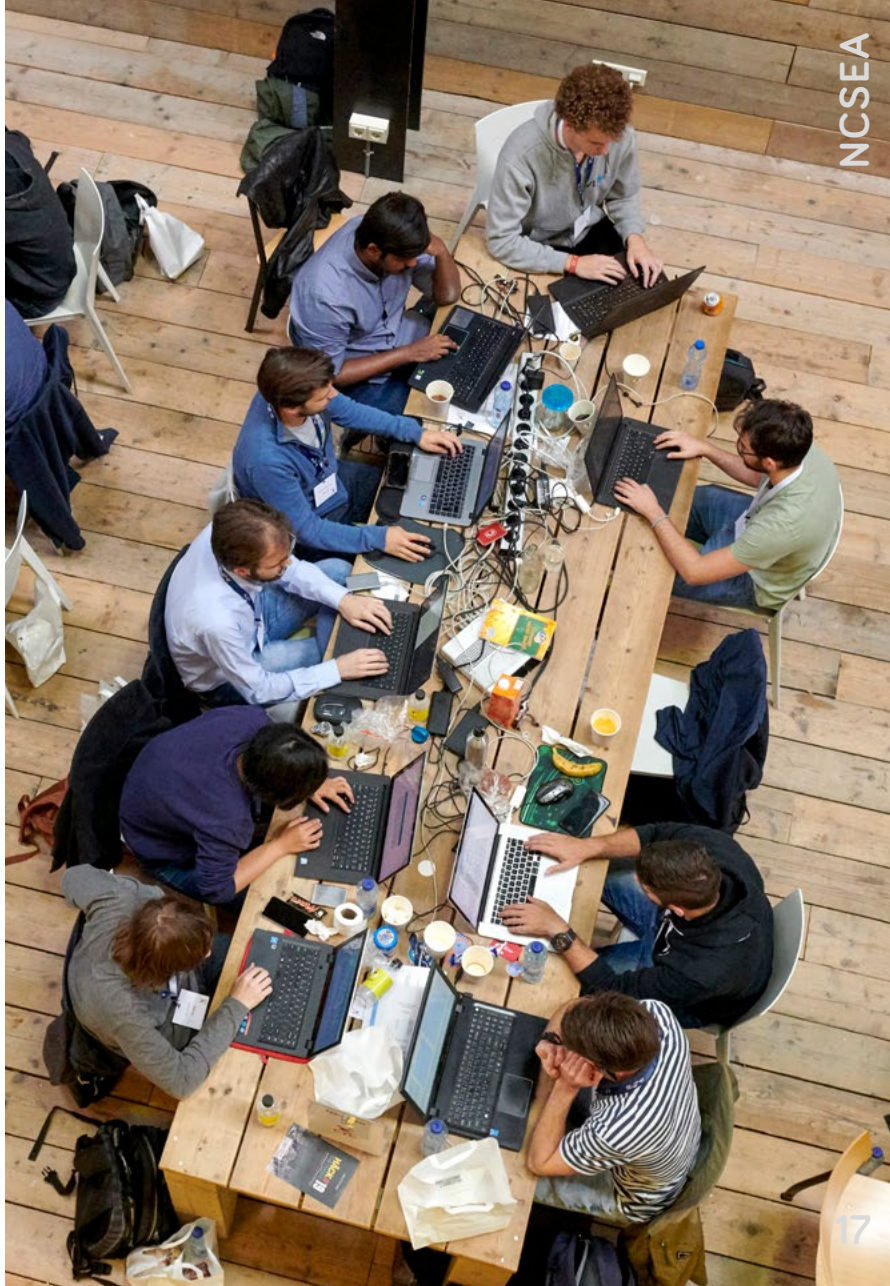
Na 20 jaar is het tijd voor een serieuze, geïntegreerde veiligheidsaanpak ten aanzien van cyberspace, opdat een veilige ruimte gecreëerd wordt voor burger en bedrijfsleven.

...

Het is tijd voor een Deltacommissaris die over alle beleidsterreinen een vorm van doorzettingsmacht heeft, die alle goede maar ontoereikende initiatieven samenbrengt en naar een hoger plan trekt. Die tegengestelde belangen oplost, richting geeft.

> "Tijd voor een Deltaplan Cyber Security" door Inge Bryan en Bibi van den Berg, 2019 [25]

De opbouw van kennis voortkomend uit de uitvoering van deze interventie-reeks vergt enkele jaren. Het opleiden van jong talent is daar onderdeel van. Dit betekent dat met de uitvoering (bijsturing en aanpassing) van deze NCSEA zo'n vijf jaar zal zijn gemoeid.



Lijst van interventies in het cybersecurity (hoger) onderwijs

De onderstaande interventies bevorderen (afzonderlijk of gezamenlijk en in samenhang) dat er voldoende afgestudeerden met de vereiste cybersecurity-kennis en -vaardigheden uitstromen uit het hoger onderwijs. Het zijn geplande en doelgerichte activiteiten, ondernomen door één of meerdere actoren, teneinde het gestelde doel te bereiken. In onderstaande figuur staan in drie kolommen respectievelijk reeds lopende én nieuwe initiatieven voor de korte én de lange termijn. Afzonderlijke interventies, of clusters van interventies, kunnen verschillende eigenaren of uitvoeringsverantwoordelijken hebben.

Door de interventies op één plaats overzichtelijk (en gerubriceerd) bijeen te brengen, wordt de samenhang zichtbaar en is afstemming mogelijk.

Elke interventie heeft een titel, een doel, de daarmee verbonden activiteiten en de toegevoegde waarde of gewenste uitkomst van de interventie. In een korte toelichting worden daarnaast de status beschreven en/of een of meerdere voorbeelden gegeven. Daarbij worden ook de betrokken organisaties (actoren) genoemd.

Figuur 2: Thematisering, samenhang en positionering in de tijd van de interventies

	Hoofdthema	Loopt	Korte termijn	Lange termijn
1	**Voorbereiden** (basis & voortgezet onderwijs = PO/VO)	CS in PO/VO curriculum; CS in NLT profiel	CS les door experts	CS in docentenopleidingen
2	**Interesseren** (kwantiteit)	CS summerschool(s)	Beroepsvoorlichting	Sterk imago; Diversiteit
3	**Professionaliseren** (CS experts)	Opleidings-overzicht; Lectoren-platform	Leven lang leren; Curriculum-gids	Gecertificeerde opleidingen; Gecertificeerde experts
4	**Doceren** (CS opleidingen)	Partnerships in education	Matchmaking platform	Bevoegde CS docenten
5	**Samenwerken** (vraag/aanbod)	Challenge the Cyber / ECSC		Nationaal; Internationaal
6	**Verbreden** (andere vakgebieden)		CS BoKS per vakgebied	CS vakbekwaamheidseisen

De interventies zijn verdeeld over zes hoofdthema's:

1. **Voorbereiden:** Veilig omgaan met de digitale infrastructuur moet van jongs af aan worden aangeleerd. Leerlingen in het primair en voortgezet onderwijs moeten les krijgen in digitale veiligheid en privacy, van docenten met cybersecuritykennis. Voor de korte termijn kunnen cybersecurity experts worden betrokken bij het geven en ontwikkelen van de lessen.
2. **Interesseren:** Op het moment van studiekeuze moet een studie cybersecurity een reële optie zijn. Een positief imago en een duidelijk beeld van het vakgebied en de loopbaanmogelijkheden, trekken meer studenten aan. Op korte termijn kan bij gevorderde (niet-cybersecurity) studenten de interesse voor cybersecurity versterkt worden.
3. **Professionaliseren:** Werkgevers, opleiders, studenten en experts hebben profijt van onafhankelijk opgestelde, uniforme, transparante eisen aan vakbekwaamheid. Met duidelijke beroepsprofielen[III] en een internationaal afgestemde Body of Knowledge and Skills (BoKS) kunnen onderwijsinstellingen vorm geven aan een curriculum dat vakbekwame experts, met up-to-date kennis en vaardigheden, opleidt.
4. **Doceren:** Er zijn meer gekwalificeerde docenten met cybersecuritykennis en -vaardigheden nodig. Op korte termijn kunnen cybersecurity experts zorgen voor kennisoverdracht in het onderwijs. Voor de lange termijn zullen meer bevoegde docenten opgeleid moeten worden.
5. **Samenwerken:** Er is regie op vraag en aanbod; periodiek monitoren onderwijsinstellingen en de arbeidsmarkt gezamenlijk de kwalitatieve en kwantitatieve behoefte en spelen daar actief op in.
6. **Verbreden:** Verbreding heeft betrekking op niet-specifieke cybersecurity-beroepen. Elke beroepsgroep stelt eisen op met betrekking tot het noodzakelijke cybersecurity-kennisniveau dat aansluit bij de beroepsuitoefening.

De vier thema's professionaliseren, doceren, samenwerken en verbreden hebben betrekking op het hoger onderwijs. De andere twee, voorbereiden en interesseren, hebben voornamelijk betrekking op het primair en voorgezet onderwijs en het mbo. Deze twee thema's moeten gezien worden als randvoorwaardelijk voor de in- en doorstroom naar het hoger onderwijs. De "summerschool" interventie is daarop een uitzondering, deze wil studenten uit het hoger onderwijs verleiden tot een vervolgstudie in cybersecurity.

III. Voor een goed begrip is het nuttig beroepsprofiel en functiebeschrijving te onderscheiden. Een beroepsprofiel geeft een formele beschrijving van een beroep. Het beschrijft de missie, taken en verantwoordelijkheden van een beoefenaar van het betreffende beroep en specificeert de competenties (kennis en vaardigheden) die de beoefenaar dient te bezitten. In een functiebeschrijving worden per werknemer rollen, verantwoordelijkheden en de vereiste kennis en vaardigheden beschreven. Het beroepsprofiel is geen functiebeschrijving, maar een beschrijving die opgenomen kan worden in een functiebeschrijving. Daarentegen is het ook mogelijk om een functie op te bouwen uit meerdere beroepsprofielen, of juist uit een deel van één beroepsprofiel.

Voorbereiden

1

De basis van digitale veiligheid

Door veiligheid en privacy in de digitale wereld op te nemen in het curriculum van het basis- en voortgezet onderwijs, raken jonge mensen vertrouwd met cybersecurity. Cybersecurity komt ook in beeld in het voortgezet onderwijs als studiekeuze. In het primair onderwijs (PO) en voortgezet onderwijs (VO) zijn daarom meer bevoegde docenten met cybersecuritykennis en -vaardigheden nodig. Om op korte termijn te voorzien in kennisoverdracht in het onderwijs, kunnen cybersecurity experts worden ingezet, onder andere voor het ontwikkelen van lesmateriaal waar PO/VO-docenten mee uit de voeten kunnen. Voor de lange termijn zullen nieuwe opleidingen voor leraren moeten worden ontwikkeld en huidige opleidingen moeten worden aangepast.

1.1. Cybersecurity in het curriculum van het primair onderwijs (PO) en voortgezet onderwijs (VO)	
Doel	Gebruik van digitale hulpmiddelen is al op jonge leeftijd gemeengoed. Per leeftijdsgroep wordt aangesloten op de aspecten van veiligheid en privacy in de digitale wereld.
Activiteiten	Het thema 'veiligheid en privacy in de digitale wereld' wordt onderdeel van het curriculum voor digitale geletterdheid in de onderbouw en bovenbouw van het PO en VO. De leermiddelen worden ontwikkeld en indien nodig bijgewerkt.
Toegevoegde waarde	Digitale veiligheid en privacy worden vanzelfsprekend voor jongeren, omdat het in het onderwijs is opgenomen. Cybersecuritykennis en -vaardigheden nemen geleidelijk toe in de maatschappij.
Toelichting	1. De afgelopen jaren is een breed, landelijk debat gevoerd over een integrale curriculumherziening in het primair, voortgezet en speciaal onderwijs. Zie SLO[26]; 2. In 2019 hebben de negen ontwikkelteams van Curriculum.nu hun voorstellen aan de minister voor Basis- en Voortgezet Onderwijs en Media overhandigd. De minister stuurt vóór de zomer van 2020 een brief aan de Tweede Kamer over de kaders voor de werkopdrachten voor het vervolgproces. Er lopen al experimenten op scholen. Zie ook: curriculum.nu.[27]

1.2. Cybersecurity als onderdeel van het keuzevak NLT in de bovenbouw van havo en vwo	
Doel	Leerlingen in de bovenbouw van havo en vwo met het profiel NLT (Natuur Leven en Technologie) ontwikkelen cybersecuritykennis, als onderdeel van de leerlijn Digitale Technologieën.
Activiteiten	Ontwikkelen en doceren van de leerlijn Digitale Technologieën, als onderdeel van het vak NLT, met cybersecurity als overkoepelend thema.
Toegevoegde waarde	Bij NLT staat voorlichting over beroepenvelden in veel modules centraal. Zo wordt bij een grote groep leerlingen kennis overgedragen én belangstelling voor het vakgebied cybersecurity gewekt.
Toelichting	1. NLT heeft een kaderstellend examenprogramma, waardoor niet jaren gewacht hoeft te worden op curriculumherzieningen of examenprogrammacommissies om het curriculum up-to-date te houden. Het Platform Talent voor Technologie en de Vereniging NLT[28] hebben hiervoor een project opgericht; 2. Zie CyBoK.org, Bringing Cyber To School: Integrating Cyber Security Into Secondary School Education[29].

1.3. Cybersecurity experts geven lessen cybersecurity in het primair onderwijs (PO) en voortgezet onderwijs (VO)	
Doel	Leerlingen in het basisonderwijs (PO) en voortgezet onderwijs (VO) leren over de aspecten van digitale veiligheid en privacy, die aansluiten bij hun leeftijdsgroep.
Activiteiten	1. Cybersecurity experts worden getraind in onderwijsvaardigheden en het eigen maken van de ontwikkelde lesstof (gebaseerd op de leerdoelen voor veiligheid en privacy in de digitale wereld van curriculum.nu); 2. Cybersecurity experts ontwikkelen, in samenwerking met PO- en VO-docenten, lesmateriaal waarmee leerkrachten zelf uit de voeten kunnen. 3. Hack in the Class geeft workshops op scholen door het hele land. Deze worden verzorgd door vrijwilligers, die het belangrijk vinden dat de jonge generatie digitaal weerbaar wordt gemaakt[30].
Toegevoegde waarde	Kinderen en jongeren ontwikkelen cybersecuritykennis en -vaardigheden die passen bij hun leeftijd. Geleidelijk nemen kennis en vaardigheden toe in de maatschappij.
Toelichting	Een werkgroep van de beroepsvereniging PvIB[31] is hiermee vergevorderd en bundelt bestaande initiatieven.

1.4. Opleiden van bevoegde docenten met cybersecurity kennis in het primair onderwijs (PO) en voortgezet onderwijs (VO)	
Doel	Bevoegde docenten in het PO en VO zijn toegerust met de benodigde cybersecuritykennis en -vaardigheden.
Activiteiten	Cybersecurity wordt opgenomen in het curriculum van de reguliere docentenopleidingen en nascholingstrajecten voor bevoegde docenten.
Toegevoegde waarde	Met docenten die kennis hebben van veiligheid en privacy in de digitale wereld, wordt het onderwerp tevens geïntegreerd in gesprekken met ouders/verzorgers.
Toelichting	Het Centre of Expertise Cyber Security (CoECS) van de Haagse Hogeschool[32] experimenteert met het opnemen van op leeftijden gerichte hulpmiddelen in het PABO curriculum.

Interesseren

2

Imago versterken en vergroten van bekendheid

Een duidelijk profiel van het veelzijdige, nog jonge vakgebied en de loopbaanmogelijkheden vergroot de kans op aanmelding van meer studenten. Jong talent wordt zo opgeleid met een duidelijke motivatie van hun studiekeuze en een duidelijk beeld van hun toekomst op de arbeidsmarkt.

2.1. Versterken van interesse voor cybersecurity bij gevorderde studenten	
Doel	Interesse stimuleren van gevorderde studenten (aan het eind van hun masteropleiding of laatste jaar van het bachelordiploma) zonder diepgaande voorkennis van cybersecurity, voor het multidisciplinaire karakter van het vakgebied.
Activiteiten	Organiseren van summerschools, waardoor studenten met interesse voor cybersecurity maar zonder diepgaande kennis daarvan, in korte tijd kennismaken met zowel technische als niet-technische aspecten van het vakgebied.
Toegevoegde waarde	Door deelnemende studenten een breed overzicht van alle onderwerpen op het gebied van cybersecurity te bieden, worden zij verleid tot een loopbaan in cybersecurity in Nederland. Dit is hiermee een van de middelen om tekorten op de Nederlandse arbeidsmarkt te verkleinen.
Toelichting	1. dcypher organiseerde van 2016 t/m 2019 jaarlijks de National Cyber Security Summer School (NCS3) voor gevorderde in Nederland studerende studenten, op initiatief van de Cyber Security Raad; 2. Europol, NATO, Universiteit Leiden, EY, Dutch Innovation Factory en HSD organiseren sinds 2015 gezamenlijk jaarlijks de International Cyber Security Summer School (ICSSS) voor (internationale) studenten en PhD-kandidaten.

2.2. Cybersecurity experts geven beroepsvoorlichting aan schoolverlaters	
Doel	Meer belangstelling voor cybersecurity opleidingen omdat het vakgebied, de status, de beroepsnormen, loopbaanmogelijkheden e.d. bekend zijn bij de bovenbouw van havo en vwo en mbo-4.
Activiteiten	1. Ontwikkelen van leermateriaal voor de bovenbouw van havo en vwo; 2. (Didactisch) getrainde cybersecurity experts verzorgen in het voortgezet onderwijs en het mbo lessen over cybersecurity onderwerpen, de inhoud en impact van het werk en de beroeps- en opleidingsmogelijkheden.
Toegevoegde waarde	Meer potentiële studenten maken een beter geïnformeerde en gemotiveerde studiekeuze, met minder tussentijdse uitval als gevolg.
Toelichting	Een werkgroep van de beroepsvereniging PvIB is hiermee vergevorderd en bundelt bestaande initiatieven.

2.3. Versterken van het imago van het vak- (en kennis-) gebied	
Doel	Een duidelijk profiel van het vakgebied en een goed overzicht van carrièrepaden en -mogelijkheden in cybersecurity, zorgen voor een gemotiveerde instroom van potentieel talent.
Activiteiten	Beroepsverenigingen definiëren, samen met bestaande programma's die gericht zijn op het enthousiasmeren van instromers, het beroepsbeeld, de loopbaanmogelijkheden en te nemen (ontwikkel)stappen.
Toegevoegde waarde	Bevordert de instroom van potentieel talent naar het cybersecurity onderwijs en wekt de interesse voor cyber-securityberoepen (in onderwijs, wetenschap, publieke en private sector).
Toelichting	Zie ook: 1. de PvIB-beroepsprofielen (gebaseerd op de EU e-CF standaard EN-16234)[33]; 2. Programma I-Partnerschap (samenwerking Rijk en Hoger Onderwijs)[34]; 3. Economic Board Zuid Holland[35].

2.4. Bevorderen van de diversiteit in cybersecurity	
Doel	Het vakgebied cybersecurity biedt gelijke kansen voor talenten met verschillende achtergronden (leeftijd, geslacht, etniciteit en cultuur) en staat bekend als divers.
Activiteiten	1. Lopende initiatieven om diversiteit te bevorderen (in Nederland en internationaal) worden geïnventariseerd; 2. Diversiteit is onderdeel van andere interventies (zoals Challenge the Cyber).
Toegevoegde waarde	Onbenut potentieel wordt aangeboord.
Toelichting	VHTO Landelijk expertisebureau meisjes/vrouwen en bèta/techniek[36] heeft ervaring met effectieve interventies om meisjes te stimuleren hun digitale vaardigheden te ontwikkelen en een toekomst in Tech/IT te verkennen, zowel binnen als buiten school. "Girlsday" is daar een markant voorbeeld van.

3

Gekwalificeerd talent voor de cybersecurity arbeidsmarkt

Het is niet direct duidelijk wat het profiel van een goede informatiebeveiliger of cybersecurity expert is. Dat maakt het voor onderwijsinstellingen niet eenvoudig om te bepalen wat de inhoud van een curriculum moet zijn. Studenten kunnen zich moeilijk een beeld vormen van wat ze willen bij het bepalen van hun studiekeuze. Voor werkgevers is het lastig om realistische verwachtingen voor starters te formuleren. Een gedragen en geaccepteerde Body of Knowledge and Skills (BoKS) helpt daarbij. Vanwege de internationale dimensie van het vakgebied is afstemming hierover noodzakelijk. Professionals moeten, indien voldaan wordt aan de eisen van opleiding, ervaring en beroepsethiek, een (inter)nationaal erkend niveau van vakbekwaamheid kunnen verwerven.

3.1. Overzicht van cybersecurity opleidingen in Nederland	
Doel	Een publiek toegankelijk actueel overzicht van cybersecurity opleidingen in Nederland, geeft inzicht in de inhoud en de samenstelling van opleidingen.
Activiteiten	1. Er wordt een eigenaar/eigenaars van de data geïdentificeerd en verantwoordelijk gesteld; 2. Het door dcypher in 2018 samengestelde overzicht wordt jaarlijks geactualiseerd en zo nodig uitgebreid.
Toegevoegde waarde	Potentiële talenten maken een beter geïnformeerde studiekeuze, werkgevers kunnen gerichter werven en selecteren en er is een basis voor informatie-uitwisseling over de inrichting van curricula.
Toelichting	Sinds 2018 houdt dcypher de gegevens bij van erkende opleidingen voor Associate degree, Bachelor en Master aan hbo en wo en publiceert de resultaten op de dcypher-website[37].

3.2. Benutten van nieuwe kennis uit (praktijkgericht) onderzoek in het hoger onderwijs	
Doel	Uitwisseling van good practices voor praktijkgericht onderzoek, samenwerking bij de inzet van onderzoeksapaciteit, krachtenbundeling bij onderzoek-aanvragen voor praktijkgericht cybersecurity onderzoek en stimuleren van de samenwerking met academische onderzoekers. Benutting van nieuwe kennis in onderwijs.
Activiteiten	HBO lectoren cybersecurity van alle relevante disciplines verenigen zich in een lectorenberaad/lectorenplatform. WO docent-onderzoekers cybersecurity verenigen zich in een soortgelijk beraad.
Toegevoegde waarde	Onderzoeksgroepen van lectoren ontwikkelen nieuwe kennis in vraaggestuurd onderzoek. Lectoren, (docent)onderzoekers en PhD's nemen kennis van actuele vraagstukken en ontwikkelingen in de maatschappij en de beroeps-praktijk. Dat komt ten goede aan de actualiteit en relevantie van de opleidingen (Bachelor en Master).
Toelichting	dcypher heeft cybersecuritylectoren van verschillende hogescholen en uit verschillende disciplines verenigd in een cybersecuritylectoren cluster (i.s.m. NRPO SIA en het landelijke Platform Praktijkgericht ICT Onderzoek PRIO[38]).

3.3. Leven lang leren	
Doel	Professionals die al in het (cyber)securitydomein werken, extra kennis en vaardigheden bieden en hoogopgeleiden (ook zonder specifieke IT-achtergrond) omscholen naar een cybersecurityfunctie.
Activiteiten	1. Ontwikkelen van programma's die hoogopgeleiden met werkervaring, met of zonder specifieke IT/cybersecurity achtergrond, opleiden voor cybersecurityfuncties. (Ook ITers moeten zonodig bijgeschoold worden. Niet elke informaticastudent is immers zomaar een expert in securitytechnologie); 2. Verder opleiden van mbo-4 afstudeerders in een duale cybersecurity opleiding.
Toegevoegde waarde	Onderwijsinstellingen dragen bij aan een leven lang leren, waardoor de mismatch op de arbeidsmarkt verkleind wordt.
Toelichting	Voorbeelden hiervan zijn: 1. Executive Master Cyber Security van de Universiteit Leiden, de TU Delft en de Haagse Hogeschool[39]; 2. Professional Master Cyber Security Engineering van de Haagse Hogeschool[40]; 3. Make IT Work[41] bij de Hogeschool van Amsterdam en NHL Stenden (Leeuwarden) voor hoogopgeleiden zonder specifieke IT-achtergrond en 4. Cloud IT Academy[42] dat mbo-ers met een afgeronde opleiding ICT of Netwerkbeheer een betaalde baan biedt in "cloud security" én een duale HBO opleiding Cyber Security & Cloud van Hogeschool Utrecht laat volgen.

3.4. Definiëren van een cybersecurity curriculum gids	
Doel	Een gids met de hoofdlijnen voor een cybersecurity curriculum wordt aan onderwijsinstellingen beschikbaar gesteld (naar het voorbeeld van het Canadian Centre for Cyber Security). Dit bevordert ook het afstemmen van curricula (mbo, hbo en wo).
Activiteiten	1. Met hulp van werkveldcommissies worden de hoofdlijnen van het onderwijsaanbod op landelijk niveau vastgelegd (incl. doorlopende leerlijnen); 2. Nieuwe relevante inzichten uit de praktijk en uit onderzoek worden vastgelegd in periodieke updates.
Toegevoegde waarde	1. Biedt een catalogus met elementen voor een curriculum; 2. Is een nationale benchmark waarmee hoger onderwijsinstellingen hun eigen programma's, lessen en leerprogramma's kunnen beoordelen; 3. Op de langere termijn kan dit leiden tot landelijke opleidingsprofielen, waarbij expliciet ruimte is voor differentiatie (aansluiting bij regionale ontwikkelingen); 4. Studenten stromen sneller door vanuit mbo-4 naar hbo en van hbo naar wo.
Toelichting	1. Zie: Joint Task Force on Cybersecurity Education, een handleiding voor het ontwerp van curricula in cybersecurity[43]; 2. Zie de Cyber Security Curriculum Guide van de Canadese Overheid[44].

3.5. Certificering van cybersecurity opleidingen	
Doel	Voor studenten en werkgevers herkenbaar maken dat opleidingen opleiden tot competenties (kennis en vaardigheden) die aansluiten bij de behoefte op de arbeidsmarkt.
Activiteiten	1. Maatschappelijke partners komen de vereiste Body of Knowledge and Skills (BoKS) overeen; 2. Erkende opleidingen, die voldoen aan de normen, worden gecertificeerd en in een register bijgehouden; 3. Cybersecurity opleidingen die qua kennis en vaardigheden voldoen aan de gestelde normen in de BoKS worden periodiek gecertificeerd.
Toegevoegde waarde	1. De startkwalificaties in het mbo, hbo en wo zijn vastgesteld; 2. Voor werkgevers is transparant welke opleidingen voldoen aan de criteria; 3. Studenten kiezen de juiste studie.
Toelichting	In de UK worden Master en Bachelor cybersecurity opleidingen gecertificeerd door NCSC-UK en GCHQ[45].

3.6. Certificering van cybersecurity experts	
Doel	Gekwalificeerde experts die voldoen aan opleidingseisen en aan maatschappelijk overeengekomen vakbekwaamheidseisen zijn (inter)nationaal herkenbaar voor de arbeidsmarkt.
Activiteiten	Implementatie van certificatie, gebaseerd op een Body of Knowledge & Skills (BoKS), beroepsprofielen en continue professionele ontwikkeling, incl. relevante kennis uit wetenschappelijk en praktijkgericht onderzoek.
Toegevoegde waarde	1. Er zijn eenduidige, transparante en uniforme normen voor vakbekwaamheid die internationaal vergelijkbaar zijn; 2. De vakbekwaamheid van experts is aantoonbaar en voldoet aan actuele eisen.
Toelichting	1. Sinds 2014 publiceert de beroepsvereniging PvIB beroepsprofielen die breed zijn geaccepteerd en die zijn gebaseerd op internationale normen (EN-16234, ISO-27000)[46]; 2. QIS heeft in publiek-private samenwerking een certificatiestelsel ontwikkeld op basis van de internationale norm voor persoonscertificatie ISO/IEC 17024.

Gekwalificeerde docenten

Er zijn meer gekwalificeerde docenten met cybersecuritykennis en -vaardigheden nodig. Op korte termijn kan een gecoördineerde actie worden opgezet, waarbij cybersecurity experts kunnen worden ingezet voor kennisoverdracht in het (hoger) onderwijs. Voor de lange termijn zullen meer bevoegde cybersecurity-docenten opgeleid moeten worden.

4.1. Partnerships in education	
Doel	Onderwijs sluit inhoudelijk optimaal aan bij de beroepspraktijk in kleine en grote organisaties en in onderwijs en onderzoek.
Activiteiten	1. Cybersecurity experts uit het bedrijfsleven en de overheid werken samen met het onderwijs om alternatieve onderwijsvormen, die stimulerend zijn voor overdracht van kennis en vaardigheden, te ontwikkelen en in de praktijk te brengen; 2. Het lectorenplatform PRIO versterkt de uitwisseling van innovatieve toepassingen uit de praktijk.
Toegevoegde waarde	Organisaties hebben een actieve rol in het verkleinen van het docententekort, terwijl afgestudeerden met up-to-date kennis en vaardigheden op de arbeidsmarkt komen.
Toelichting	Zie hiervoor onder meer de samenwerkingsvormen met het bedrijfsleven van Fontys (Partners in Education), De Haagse Hogeschool (Dutch Innovation Factory) en de Hogeschool van Utrecht (Cloud IT Academy).[47]

4.2. Matchmaking platform voor hbo- en wo-docenten	
Doel	Hbo- en wo-opleidingen beschikken over voldoende cybersecuritydocenten.
Activiteiten	Er wordt een platform opgezet om de vraag naar docenten vanuit het onderwijs en het aanbod van (gast)docenten vanuit bedrijfsleven/overheid bij elkaar te brengen.
Toegevoegde waarde	Er worden meer studenten opgeleid door meer gemotiveerde docenten. Numeri fixi als gevolg van docententekorten komen niet meer voor.
Toelichting	De Cyber Security Raad is hierover een overleg met het Ministerie van OCW gestart[48].

4.3. Opleiden van bevoegde cybersecuritydocenten met expert-kennis	
Doel	Er zijn voldoende bevoegde docenten in het mbo, hbo en wo om de benodigde (actuele) kennis en vaardigheden over te dragen aan studenten.
Activiteiten	1. De specifieke didactische en vakinhoudelijke eisen voor toekomstige hbo- en wo-docenten cybersecurity worden gedefinieerd; 2. Op basis hiervan worden het curriculum en de onderwijsmiddelen ontwikkeld; 3. Nascholingstrajecten voor bevoegde docenten worden ontwikkeld.
Toegevoegde waarde	Voldoende docenten beschikken over de kennis en vaardigheden om stimulerend les te geven en studenten te begeleiden in hun ontwikkeling, zodat opleidingen gemotiveerde en goed geëquipeerde toetreders op de arbeidsmarkt afleveren.
Toelichting	1. CyBoK, Cyber Security Body of Knowledge[49], is een open verzameling lesmateriaal gericht op WO waar universiteiten wereldwijd aan meedoen; 2. Met MOOCs (Massive Open Online Courses) zoals die van TU Delft (“Cyber Security Economics”) en Universiteit Twente (“Internet Security - Attack & Defence”) wordt kennis overgedragen aan grotere groepen studenten.

Samenwerken

Onderwijsinstellingen en de arbeidsmarkt trekken samen op

Onderwijsinstellingen en de arbeidsmarkt (koepels van werkgevers) creëren in overleg (meer) duidelijkheid over welke behoefte (kwalitatief en kwantitatief) er is aan goed voorbereide starters.

5.1. Challenge the Cyber en deelname aan de Europese landencompetitie ECSC	
Doel	1. Aanboren van nieuw en jong cybersecuritytalent (14-25 jaar); 2. Inspireren van jonge mensen om een loopbaan in cybersecurity na te streven; 3. Versterken van de afstemming van het cybersecurity onderwijs tussen mbo, hbo en wo, in samenhang met EU-landen.
Activiteiten	1. Jaarlijks organiseren van Challenge the Cyber (CtC), een Capture The Flag competitie voor jong Nederlands cybersecuritytalent (vo, mbo, hbo en wo); 2. Jaarlijks organiseren van een meerdaags cybersecuritybootcamp voor training van de grootste talenten van CtC en selectie van het Nederlandse ECSC-team; 3. Jaarlijkse deelname aan de European Cyber Security Challenge (ECSC) met 10 toptalenten; 4. Organiseren van activiteiten voor alumni en onderhouden van het netwerk.
Toegevoegde waarde	De toestroom van jong talent richting het vakgebied wordt bevorderd. Daarbij draagt de betrokkenheid van onderwijs en bedrijfsleven bij Challenge the Cyber en de aansluiting bij het Europees curriculum, bij aan de vermindering van de mismatch tussen vraag en aanbod.
Toelichting	Challenge the Cyber bestaat sinds 2019. De door het Nationaal Cyber Security Centrum en dcypher georganiseerde pilot krijgt een vervolg in 2020. Daarbij wordt nauwer samengewerkt met studenten, docenten en cybersecurity experts vanuit de overheid en het bedrijfsleven.

5.2. Evenwicht tussen cybersecurity onderwijsaanbod en arbeidsmarktvraag	
Doel	Er is, zowel in kwantitatief als kwalitatief opzicht, balans tussen de vraag naar cybersecurity experts vanuit de arbeidsmarkt en het aanbod ervan vanuit het onderwijs.
Activiteiten	1. Regionaal: vraag naar en aanbod van cybersecurity experts wordt afgestemd binnen regionale samenwerkingen tussen bedrijfsleven en onderwijs; 2. Landelijk: structureel wordt de dialoog gevoerd tussen onderwijskoepels en maatschappelijke partners om de balans op lange termijn te borgen.
Toegevoegde waarde	Een flexibele aanpak waarbij de bestaande, urgente mismatch regionaal opgelost wordt, terwijl de oplossing voor het toekomstige evenwicht tussen vraag naar en aanbod vanuit een regierol wordt belegd.
Toelichting	1. Deze interventie wordt voorbereid door een kwartiermaker; 2. De behoefte/vraag wordt gerelateerd aan het belang vanuit de samenleving (zowel economische als maatschappelijke digitale veiligheid). In veel gevallen komt dat neer op vakbekwaamheidseisen die zijn gedefinieerd door koepelorganisaties van beroepen.

5.3. Aansluiten bij internationale ontwikkelingen	
Doel	Nederland draagt in onderwijsgerelateerde gremia bij aan de wereldwijde veiligheid van de digitale samenleving.
Activiteiten	1. Er wordt kennis uitgewisseld over ontwikkelingen op het gebied van onderwijs en de gehanteerde BoKS; 2. Er wordt afgestemd over internationale programma's op het gebied van cybersecurity onderzoek, kennis en expertise, kwalificatie en certificatie.
Toegevoegde waarde	Cybersecurity houdt zich niet aan landsgrenzen en continenten. Door inzicht in en afstemming over inhoud en niveau van het onderwijs, wordt de uitwisseling van professionals bevorderd en de veiligheid van de internationale digitale samenleving verstevigd.
Toelichting	1. EU-programma's zoals CEN/e-CF, Cybersecurity4Europe, ECSO, ENISA; 2. Cybersecurity skills op de arbeidsmarkt in de UK, op basis van CyBoK[50]; 3. NIST/ National Initiative for Cybersecurity Education - NICE[51]; 4. ANSSI Frankrijk[52].

Verbreden

Cybersecurity in andere beroepen

Elke beroepsgroep stelt eisen op voor cybersecurity, die aansluiten bij de vakbekwaamheidseisen van het eigen vakgebied. Studenten krijgen tijdens hun opleiding de voor het betreffende vakgebied noodzakelijke cybersecuritykennis- en vaardigheden bijgebracht. Elke beroepsgroep houdt de cybersecurity eisen up-to-date.

6.1. Vaststellen van benodigde kennis en vaardigheden voor cybersecurity in beroepen	
Doel	De binnen beroepen noodzakelijke cybersecuritykennis en -vaardigheden zijn in kaart gebracht en actueel.
Activiteiten	1. Per beroep of vakgebied worden de noodzakelijke cybersecurity-kennis en -vaardigheden in kaart gebracht en actueel gehouden; 2. De voor een beroep of vakgebied noodzakelijke cybersecurity-kennis en -vaardigheden worden opgenomen in de relevante onderwijscurricula.
Toegevoegde waarde	Starters op de arbeidsmarkt beschikken over de voor hun vakgebied noodzakelijke cybersecuritykennis en -vaardigheden.
Toelichting	1. Fontys ICT biedt een cybersecurity minor voor studenten uit andere studierichtingen; 2. Universiteit Leiden biedt met ingang van het collegejaar 2021-2022 een cybersecurity minor voor alle LDE studenten (Universiteit Leiden, TU Delft en Erasmus Universiteit Rotterdam) met technische en sociaal-wetenschappelijke vakken; 3. Voor het vakgebied van cybersecurity experts wordt uitgegaan van beroepsprofielen en de bijbehorende BoKS.

6.2. Cybersecurity is onderdeel van vakbekwaamheids-eisen en continue ontwikkeling per beroepsgroep	
Doel	Nederlandse professionals beschikken over cybersecuritykennis en -vaardigheden die aansluiten bij verwachtingen, eisen en/of afspraken voor de beroepsuitoefening.
Activiteiten	Vak-/ beroepsverenigingen en brancheorganisaties stellen in hun vakbekwaamheidseisen het opleidingsniveau vast voor cybersecurity en zorgen ervoor dat cybersecurity wordt opgenomen in opleidingscurricula.
Toegevoegde waarde	De beroepsbevolking in Nederland is steeds vaardiger op het gebied van digitale veiligheid.
Toelichting	Voor het vakgebied van cybersecurity experts wordt uitgegaan van de eisen van vakbekwaamheid in het certificatieschema van QIS (een publiek-privaat project, zie PvIB.nl en referenties [11] en [12]).

Bijlage: Overzicht hoger onderwijs activiteiten door dcypher

Inventarisatie cybersecurity hoger onderwijs

Voor de cybersecurity sector was lang niet inzichtelijk hoe onderwijsactiviteiten kwalitatief en kwantitatief aansloten bij de vraag uit de arbeidsmarkt. In 2018 heeft dcypher het aanbod van cybersecurityopleidingen in het hoger onderwijs geïnventariseerd. Hierbij is door opleiders de studielast aangegeven voor de cybersecurityonderwerpen in hun curriculum.
Het volledige overzicht is te vinden op https://www.dcypher.nl/onderwijs. Van elke opleiding is het gedetailleerde en geactualiseerde profiel te downloaden. Dit geeft studenten, onderwijsinstellingen en werkgevers inzicht in het type opleiding. De belangrijkste bevindingen zijn:

a. er zijn twintig cybersecurityopleidingen, aangeboden door achttien onderwijsinstellingen;
b. er zijn **vijftien** voltijd opleidingen (**vijf** master, tien bachelor) en vijf deeltijd (drie master, twee bachelor);
c. dertien opleidingen zijn gericht op techniek;
d. één opleiding richt zich vooral op de organisatie van cybersecurity en één opleiding heeft de focus op mens/gedrag. Vijf opleidingen bieden een mix van de onderwerpen.

In 2018 hebben 394 studenten hun cybersecurityopleiding afgesloten met een diploma, waarvan 307 studenten met een technisch profiel. Het vinden van voldoende en de juiste docenten bleek moeilijk te zijn voor het merendeel van de opleiders.

Cybersecurity lectoren cluster

In het WO wordt al enige jaren tussen verschillende (Technische) universiteiten in de cybersecurity onderwijsprogrammering samengewerkt. Om ook de HBO opleidingen met elkaar te verbinden heeft dcypher zich ingespannen voor de oprichting van een cybersecurity lectorenberaad. Deze inspanning heeft er toe geleid dat, verbonden met Platform PRIO (Praktijkgericht ICT-Onderzoek), cybersecuritylectoren van verschillende hogescholen en uit verschillende disciplines zich hebben verenigd in een cybersecurity lectorencluster. Het doel is samenwerking, (in onderwijsprogrammering, curriculumvorming), uitwisseling van good practices en ervaringen en krachtenbundeling op het terrein van praktijkgericht cybersecurityonderzoek. Lectoren cybersecurity kunnen innovaties uit onderzoek en nieuw verworven (praktijk)kennis laten landen in het cybersecurity onderwijs. Naast ontwikkelingen uit de praktijk zorgt dat voor up-to-date en innovatief onderwijs.

Ronde tafels cybersecurity onderwijs (veldraadpleging)

In diverse Ronde Tafel bijeenkomsten en onderwijssessies tijdens dcypher symposia in de periode 2015-2017, zijn de onderwerpen en de aanpak voor een cybersecurity hoger onderwijsagenda verkend.
De aandacht voor cybersecurity in het onderwijs in het rapport 'Digitaal Droge Voeten' was aanleiding voor dcypher en het Ministerie van Justitie en Veiligheid een Ronde Tafel te organiseren (30 juni 2017). Geconstateerd werd dat economische kansen van digitalisering pas echt goed ingevuld kunnen worden als er aandacht is voor vertrouwen en veiligheid. Ook is het cybersecuritylandschap sterk gefragmenteerd, wat er toe heeft geleid dat veel spelers niet op de hoogte zijn van elkaars initiatieven. Met een gezamenlijk plan krijgen die inspanningen veel meer kracht. Een gezamenlijk opgestelde onderwijsagenda stimuleert samenwerking en verbindt verschillende initiatieven met elkaar.

National Cyber Security Summer School

Sinds 2016 organiseert dcypher jaarlijks de National Cyber Security Summer School (NCS3).
De NCS3 is een initiatief van de Cyber Security Raad (CSR). Het doel is studenten kennis te laten maken met zowel de technische als de niet-technische aspecten van cybersecurity. De zomerschool richt zich op gevorderde studenten in alle disciplines, zonder noodzakelijke cybersecuritykennis, maar wel met een dosis nieuwsgierigheid om het eigen

aandachtsgebied richting cybersecurity te verleggen. In vijf opeenvolgende dagen wordt aan studenten inzicht geboden in het brede veld, wordt cybersecurity “gedemystificeerd” en worden zij gestimuleerd zich verder vanuit hun eigen vakgebied te specialiseren in aspecten van cybersecurity. In de NCS3 opzet is een triple helix-aanpak te herkennen, waarbij kennisinstellingen, bedrijven en overheidsorganisaties worden betrokken. De NCS3 laat zien wat de verschillende sectoren doen en wat hun belang op dit gebied is. In 2019 heeft dcypher vier jaren summerschool geëvalueerd en het daaruit voortkomende evaluatierapport aan de CSR aangeboden.

Challenge the Cyber

Challenge the Cyber is een capture the flag competitie voor 14- tot 25-jarig cybersecuritytalent dat zich hiermee kan kwalificeren voor de European Cyber Security Challenge. Voor de organisatie van Challenge the Cyber (CtC) wordt samengewerkt tussen studenten en opleiders (voortgezet onderwijs, mbo, hbo en wo), overheid en private partijen. Gecoördineerd door dcypher en NCSC wordt talent bovendien getraind in technische skills, softskills en ethisch handelen in een ontwikkeltraject dat is gebaseerd op het ECSC-curriculum van het EU-agentschap ENISA. Zo ontwikkelen zich nationale en internationale communities van cybersecurity experts[53].

Gebruikte afkortingen

ANSSI	Agence nationale de la sécurité des systèmes d’information
BoKS	Body of Knowledge and Skills
CoECS	Centre of Expertise Cyber Security
CSR	Cyber Security Raad
CtC	Challenge the Cyber (dcypher/NCSC)
CyBoK	Cyber Security Body of Knowledge
dcypher	Dutch cybersecurity platform higher education & research
DIF	Dutch Innovation Factory
e-CF	e-Competence Framework
ECSC	European Cyber Security Challenge
ECSO	European Cyber Security Organisation
ENISA	European Union Agency for Cybersecurity
EHR4CYBER	European Human Resources Network for Cyber
GCHQ	Government Communications Headquarters (UK)
HCA	Human Capital Agenda
HSD	The Hague Security Delta
ICSSS	International Cyber Security Summer School
LDE	Leiden, Delft, Erasmus
MOOCs	Massive Open Online Courses
NCSA	Nationale Cyber Security Agenda (J&V)
NCS3	National Cyber Security Summer School (dcypher/CSR)
NCSRA	Nationale Cyber Security Research Agenda (dcypher)
NCSEA	Nationale Cyber Security Educatie Agenda (dcypher)
NCSC	Nationaal Cyber Security Centrum
NCTV	Nationaal Coördinator Terrorisme en Veiligheid
NLT	Natuur, leven en technologie
NICE	National Initiative for Cybersecurity Education
NIST	National Institute of Standards and Technology
NRPO SIA	Nationaal Regieorgaan Praktijkgericht Onderzoek SIA
PO	Primair Onderwijs
PRIO	Platform voor Praktijkgericht ICT Onderzoek
PvIB	Platform voor InformatieBeveiliging
QIS	Qualification scheme for Information Security professionals
SLO	Stichting Leerplan Ontwikkeling
SOC	Security Operations Center
VO	Voortgezet Onderwijs

Referenties

1. De economische en maatschappelijke noodzaak van meer cybersecurity - Nederland digitaal droge voeten, 2016
2. Roep om Gezamenlijke Onderwijsagenda, dcypher Magazine 2018 https://www.dcypher.nl/sites/default/files/uploads/magazines/dcypher-magazine-nr2-nl/mobile/index.html#p=6
3. Naar een open, veilig en welvarend digitaal Nederland - CSR-advies 2018, nr. 1 , Cyber Security Raad, 2018
4. https://www.computeridee.nl/nieuws/tno-cybercriminaliteit-kost-nederland-10-miljard/
5. Whitepaper IoT, Centrum voor Informatiebeveiliging en Privacybescherming, november 2018
6. Digitale dijkverzwaring: cybersecurity en vitale waterwerken, Algemene Rekenkamer, maart 2019
7. Cybersecuritybeeld Nederland, Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), juni 2019
8. Voorbereiden op digitale ontwrichting, Wetenschappelijke Raad voor het Regeringsbeleid, 2019
9. Kennis- en innovatieagenda (KIA) Veiligheid, oktober 2019
10. Nederlandse Cybersecurity Agenda (NCSA), Nederland digitaal veilig, Ministerie van Justitie en Veiligheid, 2018
11. Nationale Cyber Security Research Agenda - NCSRA III, dcypher, juni 2018
12. Strategische agenda hoger onderwijs en onderzoek, Ministerie van OCW, december 2019
13. • Samen aan de slag - Roadmap Human Capital 2020 - 2023 van de topsectoren, november 2019
    • Human Capital Agenda Security 2019-2022, The Hague Security Delta, 2019
14. Zie het dcypher overzicht van cybersecurity opleidingen in Nederland https://www.dcypher.nl/cybersecurity-opleidingen.
15. • De arbeidsmarkt voor cybersecurity professionals en ICT'ers, Notitie Centraal Planbureau, 2018
    • Arbeidsmarktonderzoek ICT met topsectoren, Naar een digitaal vaardiger beroepsbevolking, Berenschot, 2019
    • Onderzoek arbeidsmarkt ICT met topsectoren, CA-ICT, 2019
    • Samen aan de slag - Roadmap Human Capital 2020 - 2023 van de topsectoren, november 2019
16. • Keuzedeel mbo Security in systemen en netwerken 1 (K0400), Sectorkamer ICT en creatieve industrie, 2015
    • Keuzedeel mbo Security in systemen en netwerken 2 (K0444), Sectorkamer ICT en creatieve industrie, 2015
    • Keuzedeel mbo Veilig programmeren (K0501), Sectorkamer ICT en creatieve industrie, 2016
    • Beroepsprofielen Informatiebeveiliging beveiliging 2.0, Een basis voor uniforme kwalificatie, PvIB, 2017
17. 21st century skills: zie https://slo.nl/thema/meer/21e-eeuwsevaardigheden/
18. • European e-Competence Framework, A common European Framework for ICT Professionals in all industry sectors, CWA 16234-1, CEN
    • European ICT Professional Role Profiles, CWA part 4: Case Studies, CEN
19. • Nederlandse Cybersecurity Agenda (NCSA), Nederland digitaal veilig, Ministerie van Justitie en Veiligheid, 2018
    • Nederlandse Digitaliseringsstrategie, Ministerie van Economische Zaken en Klimaat, juni 2018
    • Defensie Cyber Strategie, Investeren in digitale slagkracht voor Nederland, Ministerie van Defensie, 2018
20. Kennis- en Innovatieagenda Sleuteltechnologieën 2020-2023, Stichting TKI HTSM, 2019, https://www.hollandhightech.nl/sites/www.hollandhightech.nl/files/inline-files/20191015%20KIA-ST.pdf
21. Missies voor het topsectoren- en innovatiebeleid, Ministerie van Economische Zaken en Klimaat, april 2019

22. • Mind the Gap: The Cyber Security Skills Shortage and Public Policy Interventions, by Tommaso De Zan, Centre for Technology and Global Affairs, University of Oxford, 2019
    • Australië, Estland, Frankrijk, Japan, Zuid Korea, Nederland, Noorwegen, Singapore, Zweden, Zwitserland, Verenigd Koninkrijk (UK), Verenigde Staten (US) *(landen die bij de ITU voorkomen in de top 20 van de ICT Development Index en de Global Cybersecurity Index)*
23. Cybersecurity skills development in the EU, ENISA, December 2019
24. https://www.ecs-org.eu/working-groups/wg5-education-awareness-training-cyber-ranges,
25. "Tijd voor een Deltaplan Cyber Security", Inge Bryan en Bibi van den Berg, 2019, https://www.deloitteforward.nl/cyber-security/tijd-voor-een-deltaplan-cyber-security/
26. Curriculum in beweging, Strategische Agenda SLO 2017 – 2020, Stichting Leerplan Ontwikkeling
27. Voorstellen voor de onderwijsinhoud van morgen, https://www.curriculum.nu/
28. https://betavak-nlt.nl/nl/p/vereniging-nlt/vereniging-nlt/
29. CyBoK.org, Bringing Cyber To School: Integrating Cyber Security Into Secondary School Education
30. Stichting Hack in the Class, https://hackintheclass.nl/
31. PvIB, https://www.pvib.nl/
32. Centre of Expertise Cyber Security (CoECS) van de Haagse Hogeschool, zie https://www.dehaagsehogeschool.nl/onderzoek/kenniscentra/details/centre-of-expertise-cyber-security
33. EU e-CF standaard EN-16234
34. Programma I-Partnerschap (samenwerking Rijk en Hoger Onderwijs) https://www.ubrijk.nl/i-partnerschap
35. Economic Board Zuid Holland, https://www.economicboardzuidholland.nl/projecten-hca/
36. VHTO Landelijk expertisebureau meisjes/vrouwen en bèta/techniek, https://www.vhto.nl/
37. Inventarisatie van erkende cybersecurity opleidingen in Nederland, PvIB Informatiebeveiliging Magazine, editie 3 2019
38. https://www.platformprio.nl/
39. https://www.csacademy.nl/educatie/masteropleidingen/executive-masteropleiding-cyber-security
40. https://www.dehaagsehogeschool.nl/opleidingen/masters/master-cyber-security-engineering
41. https://www.it-omscholing.nl/nl/
42. https://jobinthecloud.nl/
43. Cybersecurity Curricula 2017. ACM_IEEE-CS. Curriculum Guidelines, december 2017
44. Cyber Security Curriculum Guide, A role-based guide for Training and Education providers, Government of Canada, 2019
45. https://www.ncsc.gov.uk/information/ncsc-certified-degrees
46. European ICT professional role profiles, part 4: CASE STUDIES, CEN ICT Skills Workshop, 2018
47. • https://www.piefontysict.nl/nl/
    • https://www.dutchinnovationfactory.nl/
    • https://jobinthecloud.nl/
48. • CSR Adviesbrief inzake opheffing 'Numeri Fixi', Cyber Security Raad, 26 juli 2018
    • CSR Gespreksnotitie terugdringen docententekort, Cyber Security Raad, 30 augustus 2018
49. CyBoK, Cyber Security Body of Knowledge, https://www.cybok.org,
50. Cyber security skills in the UK labour market 2020, Ipsos MORI, Department for DCMS, 2020
51. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf
52. https://www.ssi.gouv.fr/uploads/2015/05/anssi_annual_report_2018_en.pdf
53. Learning by hacking, PvIB Informatiebeveiliging Magazine, editie 1 2020

Colofon

Deze agenda is tot stand gekomen in afstemming met stakeholders vanuit het hoger onderwijs, overheden en ondernemingen en in consultatie met leden van de dcypher Adviesraad.

Redactieteam
Fred van Noord
Melanie Lemmen
Jan Piet Barthel

Productie
Juul Brouwers

Ontwerp
Haagsblauw

Fotografie
Sjoerd van der Hucht

Print
Zalsman

Dit is een uitgave van dcypher, het Nederlands publiek-privaat agenderend platform voor cybersecurity onderzoek en hoger onderwijs.

dcypher

Het werk van dcypher is mogelijk gemaakt door de ministeries van OCW, J&V, EZK, Defensie en door NWO.

Rijksoverheid

31 maart 2020


dcypher